#5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Toshihisa NAKANO et al. :

Serial No. NEW : **Attn: Application Branch**

Filed December 14, 2001 : **Attorney Docket No. 2001_1837A**

KEY MANAGEMENT DEVICE/METHOD/ PROGRAM, RECORDING MEDIUM, REPRODUCING DEVICE/METHOD, RECORDING DEVICE, AND COMPUTER-READABLE, SECOND RECORDING MEDIUM STORING THE KEY MANAGEMENT PROGRAM FOR COPYRIGHT PROTECTION

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEE FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975.

CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents,
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2000-384389, filed December 18, 2000, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Toshihisa NAKANO et al.

By _____
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
December 14, 2001

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月１８日

出願番号
Application Number: 特願２０００－３８４３８９

出願人
Applicant(s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年１１月 ２日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　2022520449

【提出日】　平成12年12月18日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

H04L 12/44

G06F 13/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　中野　稔久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　松崎　なつめ

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　著作権保護データ配送方式

【特許請求の範囲】

【請求項１】　データ配送者が複数のユーザにデータを配送する著作権保護データ配送方式であって、

最上位のレイヤから最下位のレイヤまでツリー状に配置された各暗号鍵のうち、最下位の暗号鍵を個別鍵、その他の鍵をサブ鍵としたとき、

データ配送者は、全ての個別鍵と全てのサブ鍵を保持し、

各ユーザは、対応する個別鍵とそこから上位に辿った経路上に位置する１つ以上のサブ鍵を保持し、

データ配送者が、１つ以上の個別鍵あるいはサブ鍵を特定鍵として、前記特定鍵と、特定鍵から上位に辿った経路上に位置するサブ鍵をすべて無効化してデータを配送する場合、

データ配送者は、前記無効化する個別鍵あるいはサブ鍵以外であり、最も多くのユーザが共通に保持する個別鍵またはサブ鍵を決定し、決定した鍵を用いて前記データを暗号化して、暗号化に使用した鍵を特定する鍵特定情報とともに配送し、さらに前記鍵を保有していない残りのユーザがある場合には、前記の操作を繰り返し行い、

前記暗号文を受け取った各ユーザは、配送された鍵特定情報より自身が保持する個別鍵あるいはサブ鍵を決定し、決定した鍵を用いて対応する暗号文を復号して、もとのデータを獲得することを特徴とする著作権保護データ配送方式。

【請求項２】　請求項１において、

データ配送者がツリー状に配置された個別鍵とサブ鍵のセットを、2つ以上備えることを特徴とする著作権保護データ配送方法。

【請求項３】　請求項１又は請求項２記載の著作権保護データ配送方式において、

あるサブ鍵から経路を辿って1つ上位に存在する鍵をその鍵の親鍵とする場合、

データ配送者は、すべての個別鍵とサブ鍵にIDを付加し、各鍵ごとにそのIDと

親鍵のIDを鍵管理データとして保管し、さらに、親が存在しない鍵は、そのことが分かるようにして鍵管理データを保管し、

データ配送者が1つ以上の前記特定鍵と、特定鍵から上位に辿った経路上に位置するサブ鍵をすべて無効化してデータを配送する場合、

データ配送者は、無効化する暗号鍵の持つIDから、対応する鍵管理データを参照してその親鍵のIDを求め、その親鍵のIDから、対応する鍵管理データを参照して、さらにその親鍵のIDを求め、これを、親が存在しなくなるまで繰り返し行うことで、無効化する鍵を特定し、特定した無効化する鍵に対応した鍵管理データを除き、残りの鍵管理データのうち、親鍵のIDが前記無効化した鍵と一致する鍵を用いて

データを暗号化して配送することを特徴とする著作権保護データ配送方式。

【請求項４】　前記各鍵管理データは、鍵データ、鍵のID、親鍵のIDに加えて、鍵状態を示す情報を含み、鍵状態を、親が存在しない状態を最上位鍵、無効化されている状態を無効鍵、それ以外を有効鍵としたとき、

データ配送者がデータを配送するために特定鍵と、特定鍵の上位に辿った経路上に位置するサブ鍵をすべて無効化する場合、

データ配送者は、特定鍵に対応する鍵管理データの鍵状態を無効鍵に変更し、さらにその鍵管理データを参照して、親鍵のIDから得られた鍵管理データの鍵状態を無効鍵に変更し、これを、鍵状態が最上位鍵になるまで繰り返し、

また、鍵管理データに含まれる親鍵のIDのみが、前記無効鍵のIDと一致した場合、前記鍵管理データの鍵状態を、最上位鍵に変更し、

データ配送者が、前記鍵管理データから、鍵状態が最上位鍵であるものをすべて検索し、対応する鍵データを用いてデータを暗号化して配送することを特徴とする前記請求項３記載の著作権保護データ配送方式。

【請求項５】　前記鍵管理データにおいて、

初期状態における鍵状態が最上位鍵の場合は、親鍵のIDをある特定の値にすることを特徴とする前記請求項４記載の著作権保護データ配送方式。

【請求項６】　前記鍵管理データにおいて、

特定鍵からその親鍵を特定していく過程で、まず特定された鍵のIDを蓄積し、

これに基づいて、前記鍵管理データの鍵のIDが、前記特定された鍵のIDと一致しているものの鍵状態を無効鍵に変更し、

また、前記鍵管理データに含まれる親鍵のIDのみが、前記特定された鍵のIDと一致した場合、前記鍵管理データの鍵状態を最上位鍵に変更することを特徴とする前記請求項４記載の著作権保護データ配送方式。

【請求項７】　前記各鍵管理データの鍵状態として、ある特定の状態を記憶しておき、データ配送者が、データを暗号化して配送した後、前記各鍵管理データの鍵状態を記憶しておいた鍵状態に戻すことを特徴とする前記請求項４記載の著作権保護データ配送方式。

【請求項８】　前記各鍵管理データの鍵状態として記憶しておく特定の状態が複数存在し、データ配送者がデータを暗号化して配送する前に、前記各鍵管理データの鍵状態を、対象とするデータに依存していずれの鍵状態に戻すかを決定することを特徴とする前記請求項4記載の著作権保護データ配送方式。

【請求項９】　前記データ配送者がデータを暗号化して配送した後、次のデータ配送まで前記各鍵管理データの鍵状態を保持しておくことを特徴とする前記請求項4記載の著作権保護データ配送方式。

【請求項１０】　前記各鍵管理データは、鍵データ、鍵のID、親鍵のIDに加えて、鍵状態を示す情報を含み、鍵状態を、親が存在しない状態を最上位鍵、無効化されている状態を無効鍵、それ以外を有効鍵としたとき、

データ配送者が過去に排除されたユーザのうち、あるユーザのみを復帰させるために、無効化した鍵を回復する場合、データ配送者は、復帰させるユーザの回復させる鍵のIDから対応する鍵管理データを参照して、鍵状態を無効鍵から有効鍵に変更し、またその親鍵のIDを求め、さらに求めた親鍵のIDと等しい親鍵を持つ鍵を求め、その鍵の鍵管理データを参照して、鍵状態が無効鍵である場合には、回復させる鍵の鍵状態を有効鍵から最上位鍵に変更し、

データ配送者が過去に排除されたユーザのうち、あるユーザのみを復帰させてデータを配送する場合、

データ配送者は、前記鍵管理データから、鍵状態が最上位鍵であるものを全て検索し、対応する鍵データを用いてデータを暗号化して配送することを特徴とす

る前記請求項3記載の著作権保護データ配送方式。

【請求項１１】　請求項1記載の著作権保護データ配送方式において、

データ配送者が、新たにユーザを追加する場合、

追加するユーザ数に依存して、ツリー状に配置された新たな暗号鍵を作成し、その最上位の暗号鍵の親鍵を、既に存在するツリーの経路上に配置されるサブ鍵とすることを特徴とする著作権保護データ配送方式。

【請求項１２】　請求10記載の著作権保護データ配送方式において、

データ配送者が、新たにユーザを追加する場合、

追加するユーザ数に依存して、前記鍵管理データを新たに追加し、新たに追加した鍵管理データのうち、鍵状態が最上位である鍵の親鍵のIDを、既に存在する鍵管理データのうち、親鍵が最上位である鍵のIDに変更することを特徴とする著作権保護データ配送方式。

【請求項１３】　前記各ユーザは、前記暗号化されたデータとともに送られる暗号化した鍵を特定する情報を用いて、保有する個別鍵あるいはサブ鍵のいずれを用いるかを特定し、対応する暗号文を復号し、さらに、復号した結果がデータ配送者の配送したデータであることを確認する手段を有することを特徴とする請求項１記載の著作権保護データ配送方式。

【請求項１４】　データ配送者は、請求項１又は請求項2記載のすべての暗号文および、前記データを鍵として暗号化したコンテンツをメディアに蓄積してユーザに提供することを特徴とする請求項1又は請求項２記載の著作権保護データ配送方式。

【請求項１５】　前記ツリー状に配置された各暗号鍵を管理する鍵管理者を、前記データ配送者とは別に備えることを特徴とする前記請求項1記載の著作権保護データ配送方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、映画などの著作物であるコンテンツをデジタル化したデータを、例えばDVD等の可搬性の記録媒体に格納して配布する方式に関連し、同一の形態に

よりデータが記録された記録媒体により、特定のユーザ機器においてはもとのデータが獲得できず、それ以外のユーザ機器においてはもとのデータが完全に獲得できるような著作権保護データ配送方式に関する。

【０００２】

【従来の技術】

近年、蓄積メディアが大容量化するに従い、映画などの著作物であるコンテンツをデジタル化して、例えばDVD等のメディアに格納して配布するビジネスが盛んに行なわれている。このようなビジネスにおいては、プレーヤは、コンテンツの著作権を保護して、著作権者との合意による制限の下でのみコンテンツの再生や複製などを実行することが必要となる。

【０００３】

例えば、DVDにおいては、著作物を不正コピー等から保護するため、デジタルコンテンツはある暗号鍵により暗号化されＤＶＤディスクに記録され、これを復号できるのは該当する復号鍵を持つプレーヤだけといった仕組みを備えている。「Ｎａｔｉｏｎａｌ　Ｔｅｃｈｎｉｃａｌ　Ｒｅｐｏｒｔ第４３巻第３号Ｐ１１８～Ｐ１２２」（松下電器産業株式会社技術総務センター平成９年６月１８日発行）には、ＤＶＤ著作権保護システムが開示されている。

【０００４】

この場合、プレーヤの復号鍵は外部に露見しないように、厳重に管理される必要があるが、何かの事故や事件により、あるプレーヤの復号鍵が不正者に暴露されることがあるかもしれない。あるプレーヤの復号鍵が一旦不正者に暴露されてしまうと、この不正者はこれを用いてコンテンツを復号し、著作権者の制御を逃れて、コンテンツを不正に扱うかもしれない。

【０００５】

【発明が解決しようとする課題】

ところが、このＤＶＤ著作権保護システムでは、メーカごとにマスタ鍵が割り当てられているため、不正に供された特定のプレーヤだけを無効化することはできない。一旦復号鍵が暴露されると、マスタ鍵を更新することで、メーカ単位でプレーヤの無効化が図られることになる。

【０００６】

そこで、本発明は、上記課題を解決し、不正に供された特定のプレーヤだけを無効化し、他のプレーヤでは、コンテンツの再生等が可能な著作権保護データ配送方式を提供することを目的とする。

【０００７】

【課題を解決するための手段】

本発明は、上記課題に鑑み、データ配送者が複数のユーザにデータを配送する著作権保護データ配送方式であって、最上位のレイヤから最下位のレイヤまでツリー状に配置された各暗号鍵のうち、最下位の暗号鍵を個別鍵、その他の鍵をサブ鍵としたとき、データ配送者は、全ての個別鍵と全てのサブ鍵を保持し、各ユーザは、対応する個別鍵とそこから上位に辿った経路上に位置する１つ以上のサブ鍵を保持し、データ配送者が、１つ以上の個別鍵あるいはサブ鍵を特定鍵として、前記特定鍵と、特定鍵から上位に辿った経路上に位置するサブ鍵をすべて無効化してデータを配送する場合、データ配送者は、前記無効化する個別鍵あるいはサブ鍵以外であり、最も多くのユーザが共通に保持する個別鍵またはサブ鍵を決定し、決定した鍵を用いて前記データを暗号化して、暗号化に使用した鍵を特定する鍵特定情報とともに配送し、さらに前記鍵を保有していない残りのユーザがある場合には、前記の操作を繰り返し行い、前記暗号文を受け取った各ユーザは、配送された鍵特定情報より自身が保持する個別鍵あるいはサブ鍵を決定し、決定した鍵を用いて対応する暗号文を復号して、もとのデータを獲得することとしている。

【０００８】

【発明の実施の形態】

以下、本発明に係る著作権保護データ配送方式の実施の形態について図面を用いて説明する。

（実施の形態１）

図１は、本発明に係る著作権保護データ配送方式の実施の形態１の構成図である。

【０００９】

この著作権保護データ配送方式は、データ記録装置１０１と、データ記録装置１０１で暗号化されたコンテンツが記録された複数の記録媒体、例えばＤＶＤ１０２と、ＤＶＤ１０２の暗号化されたコンテンツを復号して出力する複数のプレーヤ１０３とからなる。

データ記録装置１０１は、サブ鍵・個別鍵選択部１０４と、排除鍵指定部１０５と、暗号化部１０６とを備えている。

【００１０】

サブ鍵・個別鍵選択部１０４は、図２に示すようなツリー状に配置されたサブ鍵・個別鍵を記憶している。一番下のレイヤ５の鍵を個別鍵、ツリーの経路上に存在する鍵をサブ鍵と呼ぶ。

サブ鍵・個別鍵選択部１０４は、排除鍵指定部１０５からプレーヤ（以下「ユーザ」という）７の個別鍵ＩＫ７を排除鍵として指定されると、以下のような暗号文を作成し、ＤＶＤ１０２に鍵管理情報１０７として格納する。

(1) E(IK 8、Key D')：任意に生成したKey D'をユーザ8の個別鍵で暗号化した暗号文である。ここでE(X、Y)はXを鍵としてYを暗号化した暗号文を意味し、暗号アルゴリズムとしては例えばDES暗号などの、任意の秘密鍵暗号とする。

(2) E(Key D'、Key J')：任意に生成したKey J'をKey D'で暗号化した暗号文である。

(3) E(Key C、Key J')：Key J'をKey Cで暗号化した暗号文である。

(4) E(Key J'、Key M')：任意に生成したKey M'をKey J'で暗号化した暗号文である。

(5) E(Key I、Key M')：Key M'をKey Iで暗号化した暗号文である。

(6) E(Key M'、Key O')：任意に生成したKey O'をKey M'で暗号化した暗号文である。

(7) E(Key N、Key O')：Key O'をKey Nで暗号化した暗号文である。

(8) E(Key O'、Content-Key)：コンテンツ鍵をKey O'で暗号化した暗号文である。

【００１１】

更に、各ユーザで暗号文の復号のための鍵セットを特定する鍵特定情報を格納

する。

排除鍵指定部１０５は、不正に供されたユーザ７が特定されたとき、その個別鍵ＩＫ７をサブ鍵・個別鍵選択部１０４に通知する。

暗号化部１０６は、コンテンツの入力を受け、コンテンツ鍵を用いて暗号化したコンテンツをＤＶＤ１０２に格納する。

【００１２】

ＤＶＤ１０２には、コンテンツ鍵で暗号化されたコンテンツと、暗号文からなる鍵管理情報１０７と、鍵特定情報とが記録されている。

プレーヤ１０３は、サブ鍵・個別鍵保管部１０８と、コンテンツ鍵選択部１０９と、復号部１１０とを備えている。

サブ鍵・個別鍵保管部１０８は、図２に示したツリー状の鍵のレイヤ５の個別鍵とそのツリーの経路上の上位のレイヤ１迄のサブ鍵の鍵セットを保管している。

【００１３】

例えば、ユーザ１は、個別鍵ＩＫ１と共に、その上位に位置する４つのサブ鍵（Key A, Key I, Key M, Key O）を秘密に保持している。また、ユーザ５は、個別鍵ＩＫ５と共に、その上位に位置する４つのサブ鍵（Key C, Key J ,Key M, Key O）を秘密に保管している。

コンテンツ鍵選択部１０９は、ＤＶＤ１０２から鍵管理情報１０７である暗号文と、鍵特定情報とを読み出し、サブ鍵・個別鍵保管部１０８に保管されている鍵セットから鍵特定情報で特定される個別鍵又はサブ鍵を用いて、暗号文を順次復号し、暗号化されたコンテンツ鍵を復号する。

【００１４】

例えば、ユーザ12は、自身が保持する鍵セットの中から、Key Nを用いて上記(7)の暗号文を復号し、Key O'を求めた後、これを用いて(8)の暗号文を復号してコンテンツ鍵を求める。

また、ユーザ8は、個別鍵IK 8を用いて上記暗号文(1)、(2)、(4)、(6)、(8)を順次復号して、コンテンツ鍵を求める。

【００１５】

復号されたコンテンツ鍵を復号部１１０に通知する。

なお、ユーザ７は、サブ鍵・個別鍵保管部１０８に保管されている鍵セットと鍵管理情報１０７等を用いても、コンテンツ鍵を得ることはできない。

復号部１１０は、コンテンツ鍵選択部１０９から通知されたコンテンツ鍵を用いて、ＤＶＤ１０２から読み出した暗号化されたコンテンツを復号する。復号したコンテンツを出力する。

【００１６】

このように、データ記録装置１０１の排除鍵指定部１０５で指定された個別鍵ＩＫ７を有するユーザ７では、暗号化されたコンテンツを復号することはできないので、ユーザ７を無効化することができ、他のユーザは、暗号化されたコンテンツを復号することができる。

なお、本実施の形態では、例えばツリー状の個別鍵とサブ鍵とのレイヤがＮである場合、特定の１の個別鍵を無効とするのに、鍵管理情報の暗号文は、２（Ｎ－１）個必要となる。

【００１７】

また、無効化（以下「排除」という）ユーザ以外のユーザは、場合によっては、Ｎ個の暗号文を順次復号してコンテンツ鍵を求める必要がある。

以下の実施の形態では、管理情報である暗号文を１／２とし、排除ユーザ以外のユーザは、適切なサブ鍵を用いることによって、１個の暗号文を復号するだけで、直ちにコンテンツ鍵を求めることのできる著作権保護データ配送方式について説明する。

【００１８】

また、データ記録装置１０１（以下「データ配送者」という）側でのツリーの効率の良い管理方法についても述べる。この方法を用いると排除すべき鍵から、どの鍵を用いて鍵管理情報を生成すればよいかがシステマティックに求められ、また鍵の追加も容易である。

更に、次のような不正に対して有効な対抗策も述べる。

【００１９】

不正者があるプレーヤ、例えば図2におけるユーザ７のプレーヤを不法に解析

して内部の鍵セット(IK 7、 Key D、 Key J、 Key M、 Key O)を入手したとする。

不正者は、入手した鍵セットのうち Key Oだけを内蔵した不正プレーヤを偽造する。できるだけ上位の鍵を用いることにより、流布した不正プレーヤから、どのユーザのプレーヤを解析したのかの追跡と特定が困難であるようにする。

【００２０】

図３にここで前提とするＤＶＤ１０２（以下「メディア」という）を用いた著作権保護データ配送方式のフレームワークを示す。

データ配送者は、以下の操作を行う。

(1) 任意に生成したコンテンツ鍵を用いてコンテンツを暗号化する。

(2) 無効化する鍵を指定して、コンテンツ鍵を配送するための個別鍵とサブ鍵を選択する。

(3) 選択した個別鍵とサブ鍵を用いて、それぞれコンテンツ鍵を暗号化する。

(4) コンテンツ鍵で暗号化されたコンテンツと、個別鍵あるいはサブ鍵で暗号化されたコンテンツ鍵、コンテンツ鍵を暗号化した個別鍵あるいはサブ鍵を特定する鍵特定情報をまとめてメディアに格納する。

【００２１】

一方、これを受け取ったユーザは以下の操作を行う。

(1) メディアに格納された鍵特定情報と、自身の保管している個別鍵とサブ鍵から、復号鍵を決定する。

(2) 決定した復号鍵を用いて暗号化されたコンテンツ鍵を復号する。

(3) メディアに格納されている暗号化コンテンツを、コンテンツ鍵で復号して所定のコンテンツを獲得する。

（実施の形態２）

本実施の形態では、図３における個別鍵とサブ鍵の選択と、それを用いたコンテンツ鍵の暗号化について説明する。

【００２２】

ここでは、実施の形態１と同様に、データ配送者は、図2に示す全ての個別鍵及びサブ鍵を保持し、各ユーザは、対応する個別鍵とそこから上位に辿った経路

上に位置するサブ鍵をそれぞれ保持しているものとする。また、ツリーの上位から順に、レイヤ１～レイヤ５と呼ぶことにする。このとき、レイヤ５の鍵は個別鍵となる。

【００２３】

実際に、ユーザ７の保持する鍵を全て無効化して、ユーザ7以外にデータを配送する場合の個別鍵とサブ鍵の選択と、それを用いた暗号化について、図4を参照して説明する。

図4において、ユーザ7を除くユーザの中で、最も多くのユーザが共通に保持するサブ鍵はKey Nである。次に残りのユーザの中で、最も多くのユーザが共通に保持するサブ鍵はKey Iであり、その次はKey Cである。最後、残ったユーザはユーザ8であり、その鍵は個別鍵IK 8である。よって、上記4つの鍵を用いて以下のように暗号化を行う。

(1) コンテンツ鍵をレイヤ２のKey Nを用いて暗号化する。

(2) コンテンツ鍵をレイヤ３のKey Iを用いて暗号化する。

(3) コンテンツ鍵をレイヤ４のKey Cを用いて暗号化する。

(4) コンテンツ鍵をレイヤ５のユーザ8の個別鍵IK 8を用いて暗号化する。

【００２４】

以上の(1)～(4)の暗号文と、コンテンツ鍵を用いて暗号化したコンテンツ、暗号化した鍵（Key N、Key I、Key C、IK 8）を特定するための鍵特定情報をメディアに格納する。ここで、鍵特定情報とは、例えば、それぞれの鍵に付加されているID（アルファベットあるいは数字）などがある。

これを受け取ったユーザ、例えばユーザ１は、メディアに格納されている鍵特定情報（N、I、C、8）と、自身が保持する鍵群（Key O、Key M、Key I、Key A、IK 1）から、復号鍵Key Iを決定し、これを用いて上記(2)の暗号文を復号してコンテンツ鍵を獲得し、さらにコンテンツ鍵で暗号化されたコンテンツを復号して所定のコンテンツを獲得する。このとき、復号したコンテンツ鍵を用いて直ちにコンテンツの復号を行うのではなく、まず、復号したコンテンツ鍵の正当性を確認する。ただし、この確認方法については、一般的に用いられている署名などの任意の方法とする。

【００２５】

また、例えばユーザ16は、メディアに格納されている鍵特定情報（N、I、C、8）と、自身が保持する鍵群（Key 0、Key N、Key L、Key H、IK 16）から、復号鍵Key Nを決定し、これを用いて上記(1)の暗号文を復号してコンテンツ鍵を獲得し、同様にして所定のコンテンツを獲得する。

全ての鍵を無効化されたユーザ７は、上記Key N、 Key I、 Key C、IK 8のいずれの鍵も保持していないため、コンテンツ鍵を復号することができない。

【００２６】

次に、ユーザ７に加えてユーザ12の保持する鍵を全て無効化して、ユーザ7、ユーザ12以外にデータを配送する場合の個別鍵とサブ鍵の選択と、それを用いた暗号化について、図5を参照して説明する。

図5において、ユーザ7、ユーザ12を除くユーザの中で、最も多くのユーザが共通に保持するサブ鍵はKey I、Key Lである。次に残りのユーザの中で、最も多くのユーザが共通に保持するサブ鍵はKey C、Key Eである。最後、残ったユーザはユーザ8、ユーザ11であり、その鍵は個別鍵IK 8、IK 11である。よって、上記6つの鍵を用いて以下のように暗号化を行う。

(1) コンテンツ鍵をレイヤ3のKey Iを用いて暗号化する。

(2) コンテンツ鍵をレイヤ3のKey Lを用いて暗号化する。

(3) コンテンツ鍵をレイヤ4のKey Cを用いて暗号化する。

(4) コンテンツ鍵をレイヤ4のKey Eを用いて暗号化する。

(5) コンテンツ鍵をレイヤ5のユーザ8の個別鍵IK 8を用いて暗号化する。

(6) コンテンツ鍵をレイヤ5のユーザ11の個別鍵IK 11を用いて暗号化する。

【００２７】

以上の(1)～(6)の暗号文と、コンテンツ鍵を用いて暗号化したコンテンツ、暗号化した鍵（Key I、Key J、Key C、Key E、IK 8、IK 11）を特定するための鍵特定情報をメディアに格納する。

これを受け取ったユーザ、例えばユーザ9は、メディアに格納されている鍵特定情報（I、J、C、E、8、11）と、自身が保持する鍵群（Key 0、Key N、Key K、Key E、IK 9）から、復号鍵Key Eを決定し、これを用いて上記(4)の暗号文を復

号してコンテンツ鍵を獲得し、さらにコンテンツ鍵で暗号化されたコンテンツを復号して所定のコンテンツを獲得する。

【００２８】

全ての鍵を無効化されたユーザ７、ユーザ12は、上記Key I、 Key J、 Key C、Key E、IK 8、IK 11のいずれの鍵も保持していないため、コンテンツ鍵を復号することができない。

ここでは、排除するユーザが特定できるという仮定の下で、鍵の無効化方法について説明した。ユーザが特定可能であるため、そのユーザの個別鍵から、無効化すべき全ての鍵を見つけ出すことができる。

【００２９】

一方、ユーザを特定するのが不可能な状況下で、無効化すべき鍵のみ特定している場合は、その鍵から上位に辿った経路上に位置する全ての鍵を無効化する。この特定鍵の無効化についても、上記と同様の手法により実行することが可能である。

1人のユーザを排除する場合に、本実施の形態と上記実施の形態１とを比較すると、メディアに格納される暗号文（データ量）は約1/2となる。

【００３０】

具体的には、図5及び図2におけるユーザ数16人の状態で、ユーザ7の保持する全ての鍵を無効化して、それ以外のユーザにデータを配送する場合を考える。本実施の形態においては、メディアに格納される暗号文は次の4つである。

E(Key N、Content-Key)、E(Key I、Content-Key)

E(Key C、Content-Key)、E(IK 8、Content-Key)

それに対して、上記実施の形態１においては、メディアに格納される暗号文は次の8つである。

【００３１】

E(IK 8、Key D')、　　E(Key D'、Key J')

E(Key C、Key J')、　　E(Key J'、Key M')

E(Key I、Key M')、　　E(Key M'、Key O')

E(Key N、Key O')、　　E(Key O'、Content-Key)

また、本実施の形態においては、メディアに格納された鍵特定情報から、直ちに復号鍵を特定し、1回の復号処理においてContent-Keyを得ることができる。しかし、上記実施の形態１においては、ユーザによって異なるものの、最高で5回、最低でも2回の復号処理が必要となる。ここでは、1人のユーザが保持する鍵を無効化する場合を考えたが、無効化する鍵の数が増えると、さらに本実施の形態における優位性が増すと考えられる。

【００３２】

以上より、本実施の形態においては、上記実施の形態１に比べメディアにおける記憶容量の点で有利であり、また、端末側での復号処理においても、処理回数が少なくて済むため有効な手法であると考えられる。

（実施の形態３）

本実施の形態では、2つ以上の鍵セットが存在する場合の図3における個別鍵とサブ鍵の選択と、それを用いたコンテンツ鍵の暗号化について説明する。

【００３３】

データ配送者は、図6に示す4つの鍵セットに対して、全ての個別鍵及びサブ鍵を保持し、各ユーザは、対応する個別鍵とそこから上位に辿った経路上に位置するサブ鍵をそれぞれ保持しているものとする。また、ツリーの上位から順に、レイヤ1～レイヤ3と呼ぶことにする。このとき、レイヤ3の鍵は個別鍵となる。

実際に、ユーザ７の保持する鍵を全て無効化して、ユーザ7以外にデータを配送する場合の個別鍵とサブ鍵の選択と、それを用いた暗号化について、図7を参照して説明する。

【００３４】

図7において、ユーザ7を除くユーザの中で、最も多くのユーザが共通に保持するサブ鍵は、Key I、Key K、Key Lである。次に残りのユーザの中で、最も多くのユーザが共通に保持するサブ鍵は、Key Cである。最後、残ったユーザはユーザ8であり、その鍵は個別鍵IK 8である。よって、上記5つの鍵を用いて以下のように暗号化を行う。

(1) コンテンツ鍵をレイヤ1のKey Iを用いて暗号化する。

(2) コンテンツ鍵をレイヤ1のKey Kを用いて暗号化する。

(3) コンテンツ鍵をレイヤ1のKey Lを用いて暗号化する。

(4) コンテンツ鍵をレイヤ2のKey Cを用いて暗号化する。

(5) コンテンツ鍵をレイヤ3のユーザ８の個別鍵IK 8を用いて暗号化する。

【００３５】

以上の(1)～(5)の暗号文と、コンテンツ鍵を用いて暗号化したコンテンツ、暗号化した鍵（Key I、Key K、Key L、Key C、IK 8）を特定するための鍵特定情報をメディアに格納する。ここで、鍵特定情報とは、例えば、それぞれの鍵に付加されているID（アルファベットあるいは数字）などがある。

これを受け取ったユーザ、例えばユーザ１は、メディアに格納されている鍵特定情報（I、K、L、C、8）と、自身が保持する鍵群（Key I、Key A、IK 1）から、復号鍵Key Iを決定し、これを用いて上記(1)の暗号文を復号してコンテンツ鍵を獲得し、さらにコンテンツ鍵で暗号化されたコンテンツを復号して所定のコンテンツを獲得する。

【００３６】

また、例えばユーザ6は、メディアに格納されている鍵特定情報（I、K、L、C、8）と、自身が保持する鍵群（Key J、Key C、IK 6）から、復号鍵Key Cを決定し、これを用いて上記(4)の暗号文を復号してコンテンツ鍵を獲得し、同様にして所定のコンテンツを獲得する。

全ての鍵を無効化されたユーザ７は、上記Key I、 Key K、 Key L、Key C、IK 8のいずれの鍵も保持していないため、コンテンツ鍵を復号することができない。

【００３７】

本実施の形態においては、上記実施の形態２に比べて、以下の点で有利である。

第１に、データ配送者の鍵管理データのデータ量が少ない。本実施の形態（図6）と上記実施の形態２（図2）とを比較した場合、同一ユーザ数（ユーザ数16人）であるにも関わらず、鍵の総数は、本実施の形態が28個であるのに対し、上記実施の形態２では31個である。このことより、本実施の形態は、データ配送者における鍵の記憶容量、鍵管理の容易さの点から優位性があると考えられる。

【００３８】

第２に、各ユーザが保持する鍵データのデータ量が少ない。

本実施の形態（図6）と上記実施の形態2（図2）とを比較した場合、各ユーザが保持する鍵の総数は、本実施の形態が3個であるのに対し、上記実施の形態２では5個である。このことより、本実施の形態は、ユーザにおける記憶容量の点から優位性があると考えられる。

【００３９】

また、ユーザが保持する鍵の総数が少ないことは、あるユーザが不正に解析され、内部に保持している鍵が不正者に入手された場合においてもリスクが低いと考えられる。

これは、次のようなアタックに対するリスクを想定している。

(1) 不正者はあるユーザを解析し、不正に全ての鍵を入手する。

(2) 不正者は、入手した鍵の最上位の鍵のみを組み込んだクローンユーザ（不正なプレーヤ）を生成する。

(3) クローンユーザを発見したデータ配送者は、その中に組み込まれている鍵（最上位の鍵）を無効化して、データ配送を行う。

(4) 不正者は、次は無効化された鍵の1つ下位の鍵のみを組み込んだクローンユーザを生成する。

(5) クローンユーザを発見したデータ配送者は、その中に組み込まれている鍵を無効化して、データ配送を行う。

(6) 以降、データ配送者と不正者の間で(1)～(5)が繰り返され、最終的には、不正に解析されたユーザを特定することができる。

【００４０】

上記のようなアタックでは、データ配送者と不正者との攻防が、不正者が入手した鍵の数だけ続くことになる。このため、ユーザに格納される鍵の数が少なければ少ないほど、不正者に入手される鍵の数も少なくなり、上記アタックによる被害も軽減されるため、鍵セットの数を増やす必要がある。

しかし、鍵セットの数を増やすと、無効化されている鍵が少ない状態において、暗号文の数が増加してしまう。具体的には、いずれの鍵も無効化されていない

状態において、実施の形態2（図2）では、暗号文が1つであるのに対し、本実施の形態（図5）では、暗号文が4つ必要となる。
以上のことより、第2の実施の形態においては、鍵セットの個数と無効化する鍵（排除するユーザ）の数が重要なファクターとなる。

【００４１】

ここでは、暗号文の最大データ量を見積もるために、排除ユーザの上限を設定し、上限までユーザが排除されており、また、ツリーが最も細かく分断されるようにユーザは排除されているものと仮定する。

例えば図5において、ユーザ7とユーザ12の2人を排除した場合、Key O、Key M、Key Nが無効化されていることから、図6に示すような鍵セットが4つ存在する場合と同じ状態であると考えられる。よって、排除ユーザの上限を2人とした場合では、鍵セットの個数が4つまでであるなら、暗号文の最大データ量は等しいと考えられる。逆に、4つ以上、例えば鍵セットを8つにした場合には、余分なツリーの分割を行っていることになるため、暗号文のデータ量が増加すると考えられる。

【００４２】

以上のことより、排除するユーザの上限を2nとした場合、鍵セットの数が、鍵セット数≦2n+1であるなら暗号文の最大データ量は等しいと考えられる。また、各ユーザの保持する鍵の数が少なければ、想定しているアタックのリスクも軽減されるため、排除するユーザ数の上限が2nの場合においては、鍵セットの数は2n+1個が最適であると考えられる。

【００４３】

ただし、鍵セットを分割した場合、排除するユーザ数が上限に達するまでは、鍵セットが1つの場合に比べ、暗号文のデータ量が増えてしまう。しかし、排除ユーザ数の上限を設定しており、その時の最大データ量が等しく、大容量のメディアにはその領域が確保されているため、実用上は問題ないものと考えられる。

（実施の形態4）

データ配送者は、上記実施の形態2及び実施の形態3において無効化する鍵を決定後、その鍵以外であり、最も多くのユーザが共通に保持するサブ鍵を選択し、

さらに残りのユーザがある場合はこの操作を繰り返し行わなければならない。

【００４４】

本実施の形態では、データ配送者が、この暗号化鍵をシステマティックに決定できる鍵管理方法について説明する。

データ配送者もしくは別の鍵管理者は、図2においてツリー状に配置された全ての個別鍵とサブ鍵を保持している。このとき、各鍵は鍵データ、鍵のID、親鍵のID、鍵状態を示す情報を、図8に示す鍵管理データとして保有する。ただし、親が存在しない最上位に位置する鍵（図2におけるKey 0）は、鍵データ、鍵のID、親が存在しないことを示す情報（ここでは数値"11…11"と仮定）、鍵状態を示す情報を、同じく鍵管理データとして保有する。鍵状態を示す情報については、ここでは、最上位鍵（暗号化するための鍵）を"1"、無効鍵を"-1"、それ以外の有効鍵を"0"と表現する。

【００４５】

実際に、ユーザ７の保持する鍵を全て無効化して、ユーザ7以外にデータを配送する場合の個別鍵とサブ鍵の選択方法について、図9を参照して説明する。また、図10には鍵の無効化方法のフローチャートを示す。

＜ユーザ7が保持する鍵の無効化方法＞

(1) ユーザ7の個別鍵（IK 7）の鍵管理データから、親鍵のID（Key D）を取得する。

(2) 取得した鍵のID（Key D）の鍵管理データから、その親鍵のID（Key I）を取得する。

(3) 取得した鍵のID（Key I）の鍵管理データから、その親鍵のID（Key M）を取得する。

(4) 以降、(1)～(3)の操作を親が存在しないことを示す値"11…11"を取得するまで繰り返し行い、その間に取得した鍵のIDを記憶しておく。

(5) 記憶した無効化する鍵のIDをもとに、鍵セットにおける全ての鍵管理データの探索を行い、

(ア) 鍵のIDが無効化する鍵と一致した場合、鍵状態を示す情報を"-1"に変換する。

（イ）親鍵のIDのみが無効化する鍵と一致した場合、鍵状態を示す情報を"1"に変換する。

（ウ）例外として、すでに鍵状態を示す情報が"-1"であるものについては、上記（ア）、（イ）の操作は行わないものとする。

＜暗号化するための鍵の選択方法＞

(1) 更新された鍵セットの中から、鍵状態が"1"を示す個別鍵及びサブ鍵を探索する。図9において、初めて決定されるサブ鍵（暗号化鍵）はKey Nである。

(2) 暗号化鍵は2つ以上存在する可能性があるため、続けて探索を行い全ての暗号化鍵を決定する。図9では、Key N、Key I、Key C、IK 8が暗号化鍵として決定される。

【００４６】

データ配送者は、上記方法で取得した暗号化鍵を用いてコンテンツ鍵を暗号化して、各ユーザに配布する。

ここでは、鍵セットが1つの場合の例を用いて説明したが、データ配送者が2つ以上の鍵セットを保有する場合においても、個々の鍵セットに対して同様の方法を実行することで暗号化鍵を決定及び管理することができる。

【００４７】

暗号化鍵の決定後あるいは暗号化前に、データ配送者は保有する鍵管理データについて、

・ 鍵状態を初期状態に戻す。
・ 鍵状態を過去のある状態にまで戻す。
・ 鍵状態をそのまま保持する。

の3つパターンが考えられる。

＜鍵状態を初期状態に戻す＞

鍵状態を初期状態に戻すとは、鍵管理データ内の鍵状態を、いずれの鍵も無効化されていない状態に戻すことである。すなわち、図9の左側に示すように、一つの鍵についてのみ鍵状態が"1"であり（図9におけるKey 0）、それ以外は全て"0"であるような状態のことである。

常に鍵管理データが初期状態にあることから、例えばメディアに格納するコンテ

ンツ毎に配送するユーザを変更したい場合などに対してはフレキシブルに対応可能である。

＜鍵の状態を過去のある状態にまで戻す＞

あるユーザもしくはある鍵を永久に無効化している状態で、上記のようにコンテンツ毎にフレキシブルに対応可能である。

過去のある状態に戻す場合、戻したい過去の状態を記憶しておき、例えばその状態の無効鍵及び最上位鍵をリストとして保持しておき、暗号化鍵を決定後あるいは暗号化前に、そのリストを用いて、常にある状態に戻すようにする。

＜鍵の状態をそのまま保持する＞

無効化する鍵が増加してきた場合、鍵の状態をそのまま保持することで、新たな無効化鍵が出てきた場合においても、保持する鍵の状態からの変更で済むため、暗号化鍵の決定が比較的容易に実行可能である。

【００４８】

この暗号化鍵の決定方法は上記に示した通りである。

（実施の形態5）

上記実施の形態4において、暗号化鍵を決定後、鍵の状態をそのまま保持し続ける場合において、本実施の形態では、データ配送者が、過去に無効化したある特定の鍵を、それ以外の鍵を無効化したまま、システマティックに回復させることができる鍵管理方法について説明する。

【００４９】

データ配送者は、図2に示す全ての個別鍵及びサブ鍵を保持し、各ユーザは、対応する個別鍵とそこから上位に辿った経路上に位置するサブ鍵をそれぞれ保持しているものとする。

実際に、図5のようにユーザ７、ユーザ12が排除されており、鍵管理データが保持されているという仮定の下で、ユーザ12の鍵を無効化しつつ、ユーザ7の鍵を回復させる場合において、個別鍵とサブ鍵の選択と、それを用いた暗号化について図11を用いて説明する。 また、図12には鍵の回復方法のフローチャートを示す。

＜ユーザ7が保持する鍵の回復方法＞

(1) ユーザ7の個別鍵の鍵管理データから、親鍵のID（Key D）を取得する。
(2) 取得した鍵のID（Key D）の鍵管理データから、その親鍵のID（Key I）を取得する。
(3) 取得した鍵のID（Key I）の鍵管理データから、その親鍵のID（Key M）を取得する。
(4) 以降、(1)～(3)の操作を親が存在しないことを示す値"11…11"を取得するまで繰り返し行い、その間に取得した鍵のIDをユーザ7の保持する鍵として記憶しておく。
(5) ユーザ7の保持する鍵のIDをもとに、鍵セットにおける全ての鍵管理データの探索を行い、
（ア）鍵のIDが、ユーザ7の鍵と一致した場合、その鍵と同じ親を持つ他の鍵を探索する。
（イ）同じ親をもつ鍵の鍵管理データにおける鍵の状態が、無効鍵を示す"-1"であるならば、(ア)で一致した鍵の鍵管理データにおける、鍵の状態を最上位鍵を示す"1"に変換する。
＜暗号化するための鍵の選択方法＞
(1) 更新された鍵セットの中から、鍵自身の状態が"1"を示す個別鍵及びサブ鍵を探索する。図11において、初めて決定されるサブ鍵（暗号化鍵）はKey Mである。
(2) 暗号化鍵は2つ以上存在する可能性があるため、続けて探索を行い全ての暗号化鍵を決定する。図11では、Key M、Key L、Key E、ユーザ11の個別鍵が暗号化鍵として決定される。

【００５０】

データ配送者は、上記方法で取得した暗号化鍵を用いてコンテンツ鍵を暗号化して、各ユーザに配布する。

ここでは、鍵セットが1つの場合の例を用いて説明したが、データ配送者が2つ以上の鍵セットを保有する場合においても、個々の鍵セットに対して同様の方法を実行することで暗号化鍵を決定することができる。

（実施の形態6）

本実施の形態では、データ配送者が、特定のユーザを排除しつつ新たに複数のユーザを追加する方法について図13を参照にして説明する。

【００５１】

ここでは、図4に示すユーザ7が排除されている状態において、8人のユーザを新たに追加する場合を考える。

(1) データ配送者は、新たに追加する8人について、最上位のレイヤから最下位のレイヤまでツリー状に配置された新たな鍵セットを構成し、全ての個別鍵とサブ鍵を保持する。

(2) 既存の鍵セットの中から鍵状態が"1"を示す鍵を選択する。例として図13では、Key Nを選択する。

(3) (2)で探索したサブ鍵を、(1)で構成した鍵セットの最上位に位置するサブ鍵の親とする。

【００５２】

以上、(1)～(3)に述べた方法により、新たなユーザの追加が可能である。

以下では、データ配送者が、上記の方法により新たにユーザを追加した場合において、鍵を追加する鍵管理方法について説明する。

データ配送者は、図13に示す既存の鍵セット及び新たに追加作成した鍵セットの個別鍵及びサブ鍵を保持し、各ユーザは、対応する個別鍵とそこから上位に辿った経路上に位置するサブ鍵をそれぞれ保持しているものとする。

【００５３】

新たに作成された鍵セットの最上位に位置する鍵（図13ではKey R）の親鍵のIDは、親が存在しないことを示す“11…11”である。ここで、既存の鍵セットの中から鍵状態が"1"を示す鍵を選択し（図13では、Key Nを選択したと仮定）、新たに作成した鍵セットの最上位鍵（Key R）の親鍵のID（“11…11”）を、選択した鍵のID（Key N）に変更する。これにより、新たに作成した鍵セットが既存の鍵セットに追加される。

ただし、既存の鍵セットの中から鍵状態が"1"を示す鍵を選択するときは、前記条件が満たされていれば、任意の鍵を選択することが可能である。

【００５４】

なお、以上述べた本発明に係る著作権保護データ配送方式の実施の形態では、データ量の多いコンテンツを想定し、コンテンツ鍵でコンテンツを暗号化し、さらに、各サブ鍵あるいは個別鍵でコンテンツ鍵を暗号化するといった、２階層構造を考えたが、コンテンツ自身のデータ量が少ない場合には、各サブ鍵あるいは個別鍵で直接コンテンツを暗号化しても良い。

【００５５】

また、以上の実施の形態では、１つの経路から２つに分岐するバイナリツリーを例として用いたが、この分岐の数は分岐ごとに異なっていても良いし、３以上であってもよい。

【００５６】

【発明の効果】

以上の説明から明らかなように、本発明に係る著作権保護データ配送方式は、特定のユーザだけを無効化することができる。

また、請求項2に係る発明においては、鍵の総数が少ないことから、データ配送者の鍵管理データのデータ量及び各ユーザが保持する鍵データのデータ量が少なくて済む。さらに、各ユーザが保持する鍵データが少ないことは、記憶容量の点で有利であるのにくわえて、想定するアタックに対してもリスクを軽減できると考えられる。

【図面の簡単な説明】

【図1】

本発明に係る著作権保護データ配送方式の実施の形態１の構成図である。

【図2】

上記実施の形態のデータ記録装置のサブ鍵・個別鍵選択部に記憶されたツリー状に配置した鍵の構成を示す論理図である。

【図3】

本発明に係る著作権保護データ配送方式の実施の形態2のフレームワークを説明する図である。

【図4】

上記実施の形態において、1人のユーザを排除するときのサブ鍵と個別鍵の選

択およびこれらによるコンテンツ鍵の暗号化を説明するための論理図である。

【図5】

上記実施の形態において、2人のユーザを排除するときのサブ鍵と個別鍵の選択およびこれらによるコンテンツ鍵の暗号化を説明するための論理図である。

【図6】

本発明に係る著作権保護データ配送方式実施の形態3において、ツリー状に配置したサブ鍵の構成を示す論理図である。

【図7】

上記実施の形態において、1人のユーザを排除するときのサブ鍵と個別鍵の選択およびこれらによるコンテンツ鍵の暗号化を説明するための論理図である。

【図8】

本発明に係る著作権保護データ配送方式の実施の形態4における、鍵管理データの模式図である。

【図9】

上記実施の形態において、鍵管理を行うときの模式図である。

【図10】

上記実施の形態において、鍵管理を行うときのフローチャートである。

【図11】

本発明に係る著作権保護データ配送方式の実施の形態5において、鍵管理を行うときの模式図である。

【図12】

上記実施の形態において、鍵管理を行うときのフローチャートである。

【図13】

本発明に係る著作権保護データ配送方式の実施の形態6において、ツリー状に配置したサブ鍵の構成を示す論理図である。

【符号の説明】

１０１　データ記録装置

１０２　ＤＶＤ

１０３　プレーヤ

１０４　サブ鍵・個別鍵選択部

１０５　排除鍵指定部

１０６　暗号部

１０７　鍵管理情報

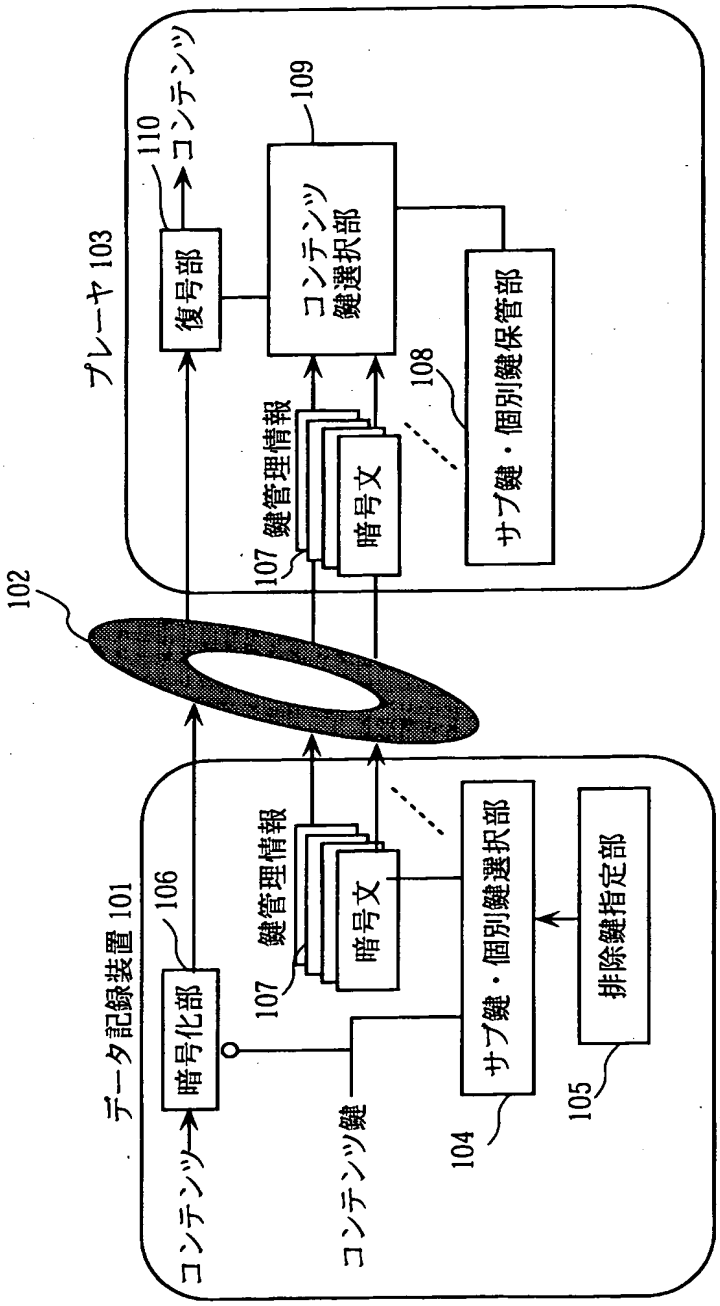
１０８　サブ鍵・個別鍵保管部

１０９　コンテンツ鍵選択部

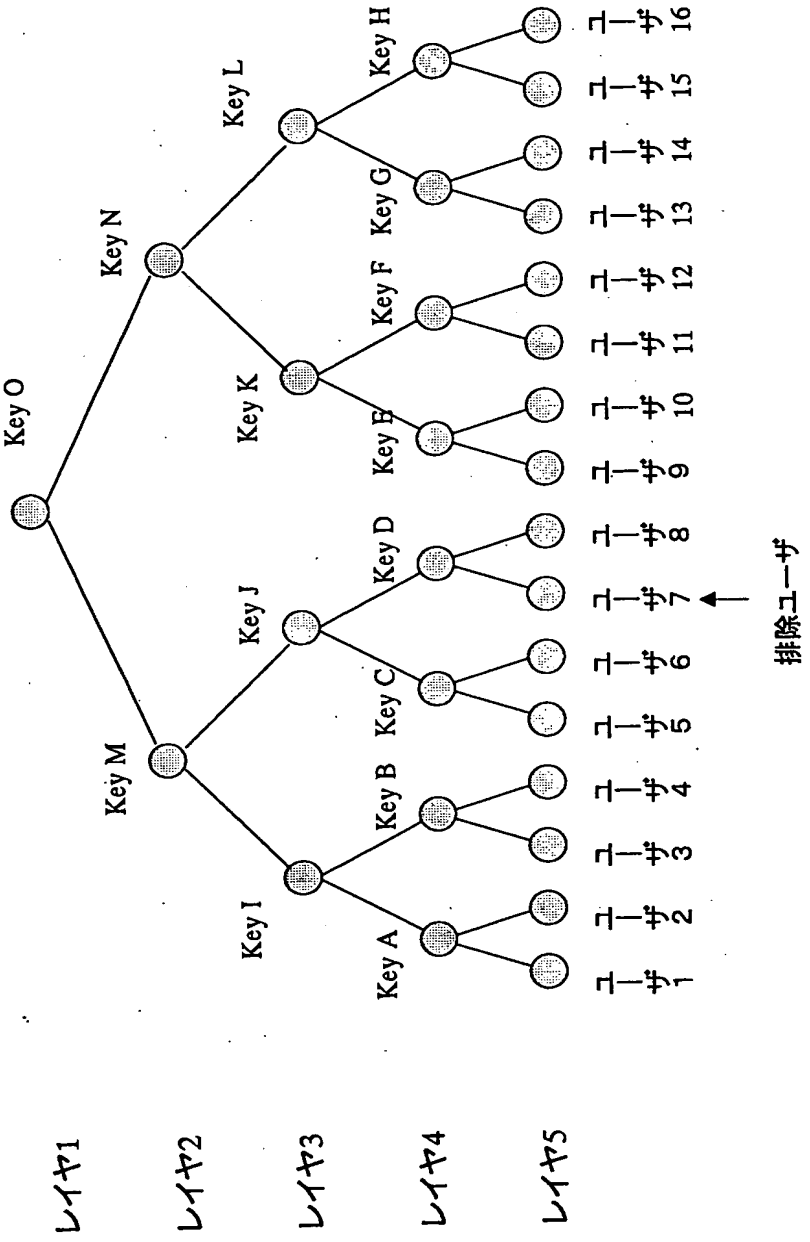
１１０　復号部

【書類名】　　図面

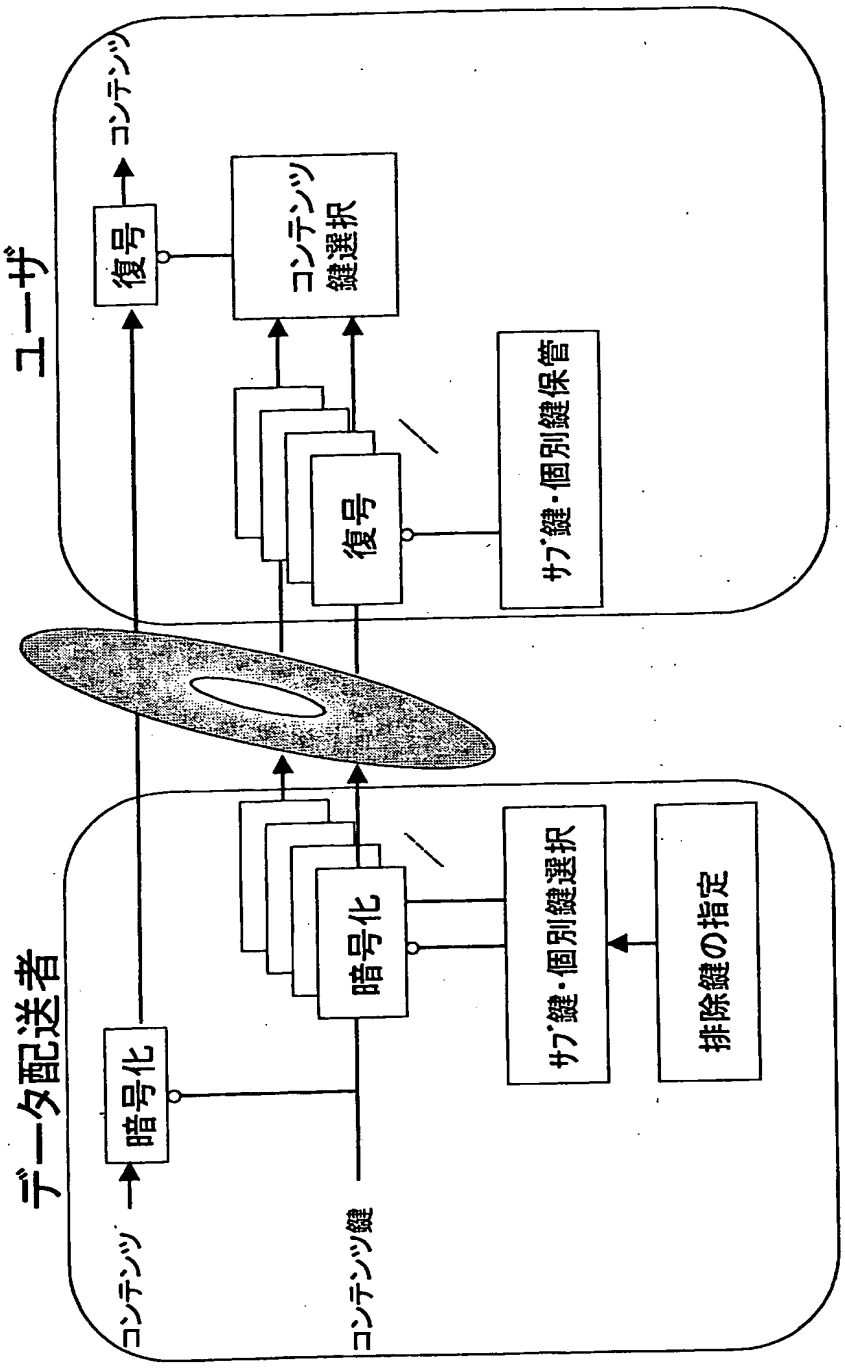
【図１】


データ記録装置 101
コンテンツ
暗号化部
106
コンテンツ鍵
107
鍵管理情報
暗号文
サブ鍵・個別鍵選択部
104
排除鍵指定部
105
102
プレーヤ 103
復号部
110
コンテンツ
コンテンツ鍵選択部
109
108
サブ鍵・個別鍵保管部

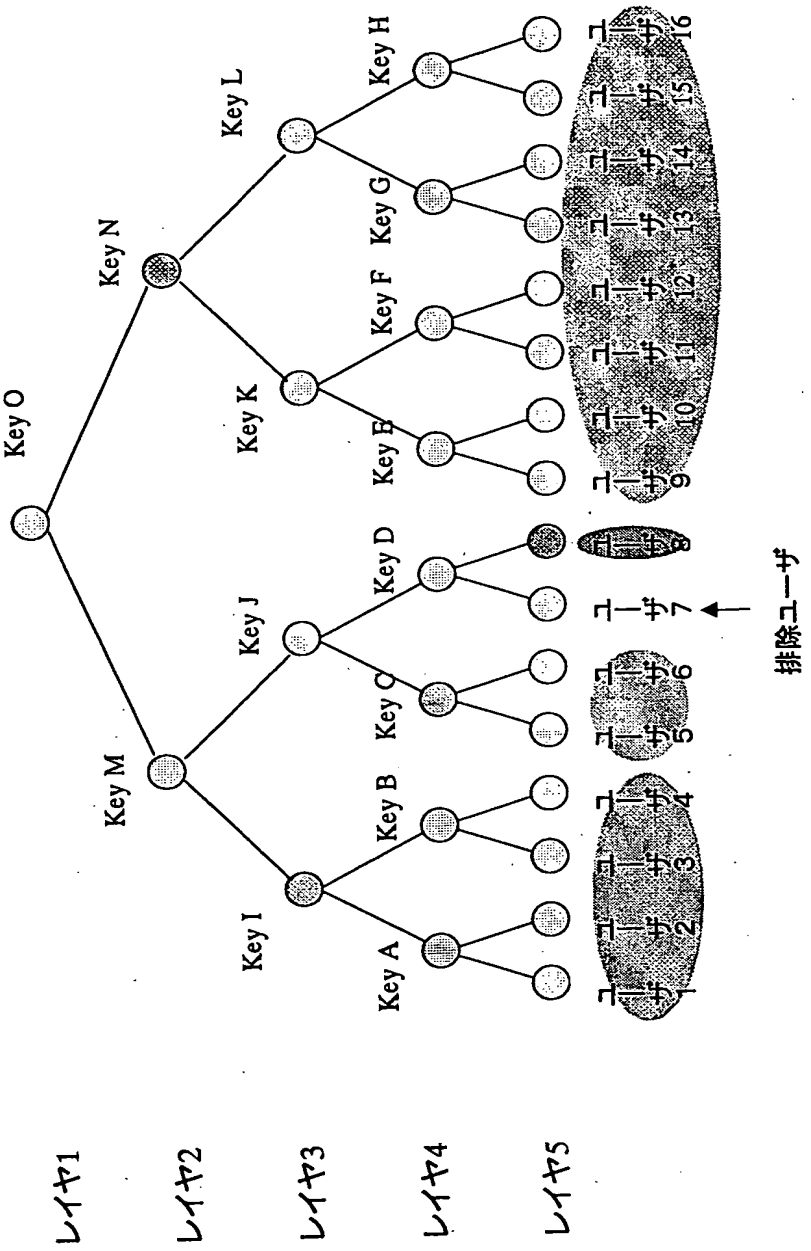
【図２】


Key O
Key N
Key M
Key L
Key K
Key J
Key I
Key H
Key G
Key F
Key E
Key D
Key C
Key B
Key A
ユーザ 1
ユーザ 2
ユーザ 3
ユーザ 4
ユーザ 5
ユーザ 6
ユーザ 7
ユーザ 8
ユーザ 9
ユーザ 10
ユーザ 11
ユーザ 12
ユーザ 13
ユーザ 14
ユーザ 15
ユーザ 16
排除ユーザ
レイヤ1
レイヤ2
レイヤ3
レイヤ4
レイヤ5

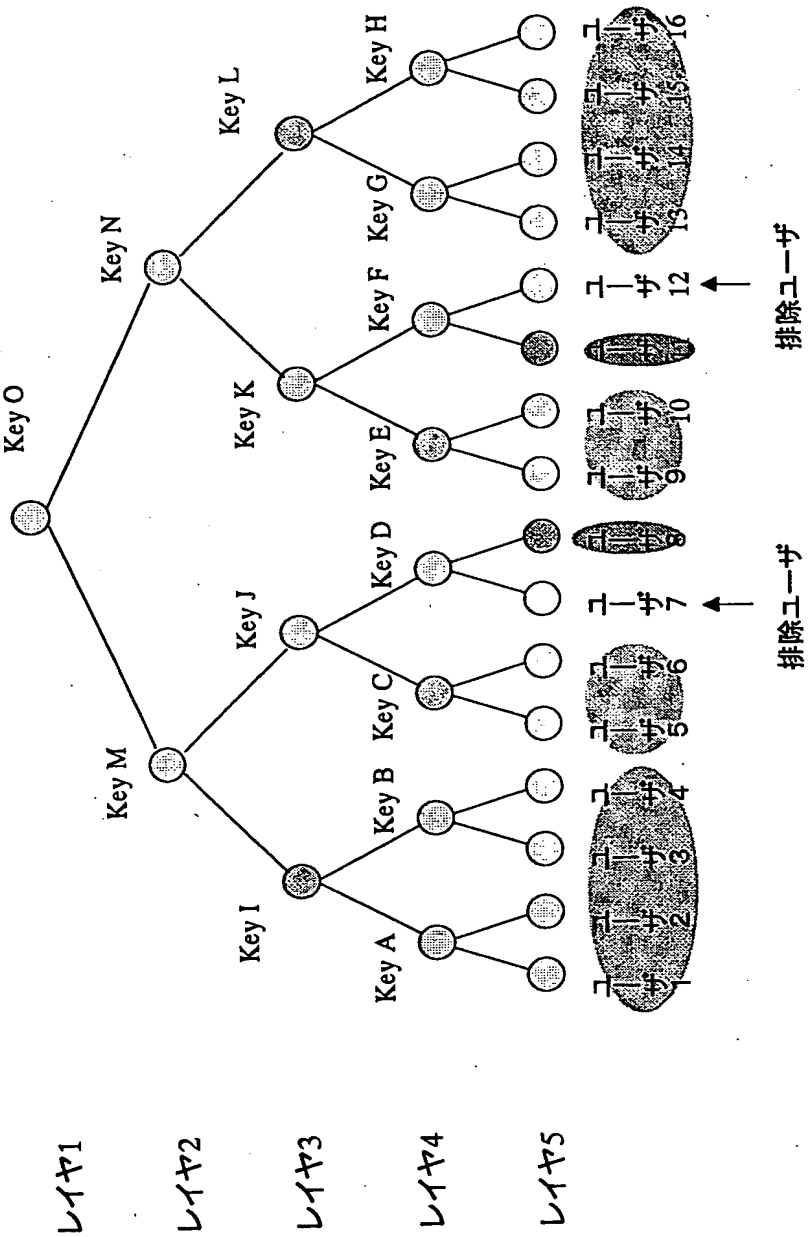
【図３】


ユーザ
コンテンツ
復号
コンテンツ鍵選択
復号
サブ鍵・個別鍵保管
データ配送者
コンテンツ
暗号化
コンテンツ鍵
暗号化
サブ鍵・個別鍵選択
排除鍵の指定

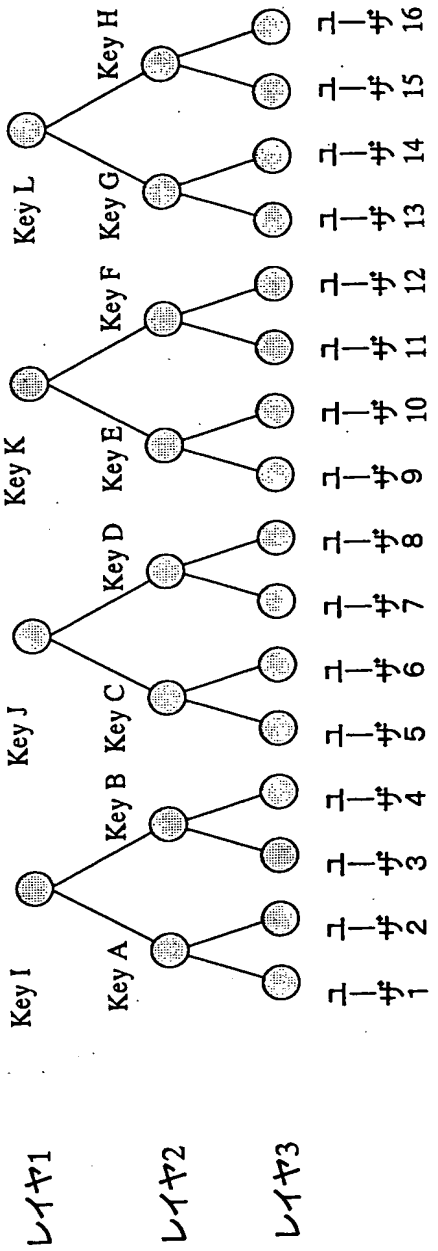
【図４】


Key O
Key N
Key M
Key L
Key K
Key J
Key I
Key H
Key G
Key F
Key E
Key D
Key C
Key B
Key A
ユーザ 1
ユーザ 2
ユーザ 3
ユーザ 4
ユーザ 5
ユーザ 6
ユーザ 7
ユーザ 8
ユーザ 9
ユーザ 10
ユーザ 11
ユーザ 12
ユーザ 13
ユーザ 14
ユーザ 15
ユーザ 16
排除ユーザ
レイヤ1
レイヤ2
レイヤ3
レイヤ4
レイヤ5

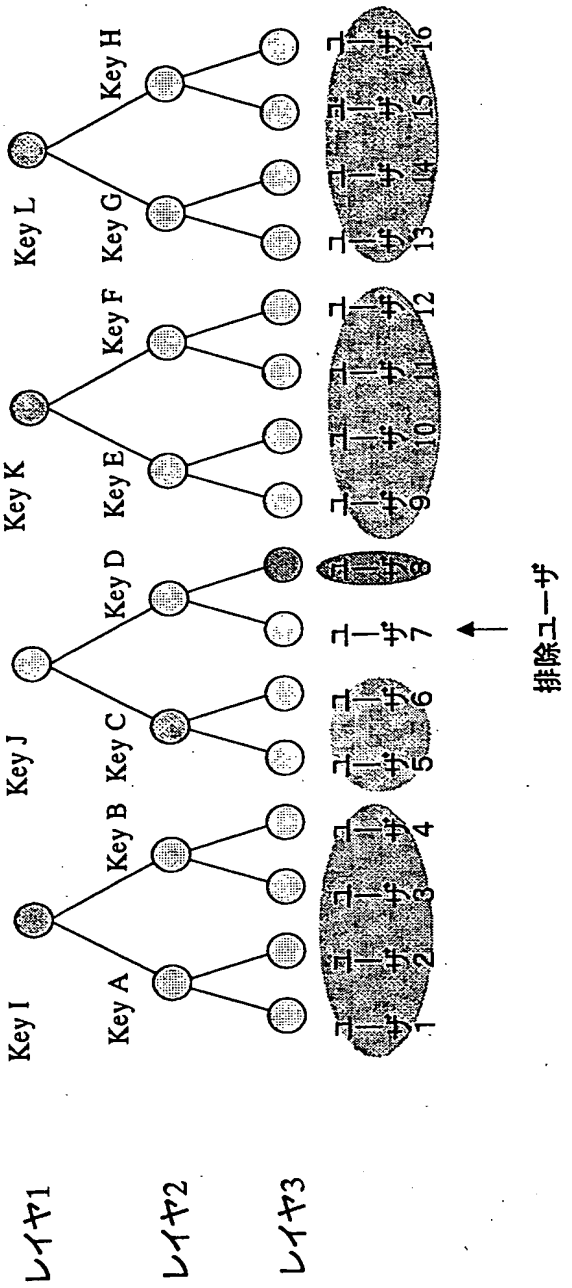
【図５】


Key O
Key N
Key M
Key L
Key K
Key J
Key I
Key H
Key G
Key F
Key E
Key D
Key C
Key B
Key A
ユーザ1
ユーザ2
ユーザ3
ユーザ4
ユーザ5
ユーザ6
ユーザ7
ユーザ8
ユーザ9
ユーザ10
ユーザ11
ユーザ12
ユーザ13
ユーザ14
ユーザ15
ユーザ16
排除ユーザ
排除ユーザ
レイヤ1
レイヤ2
レイヤ3
レイヤ4
レイヤ5

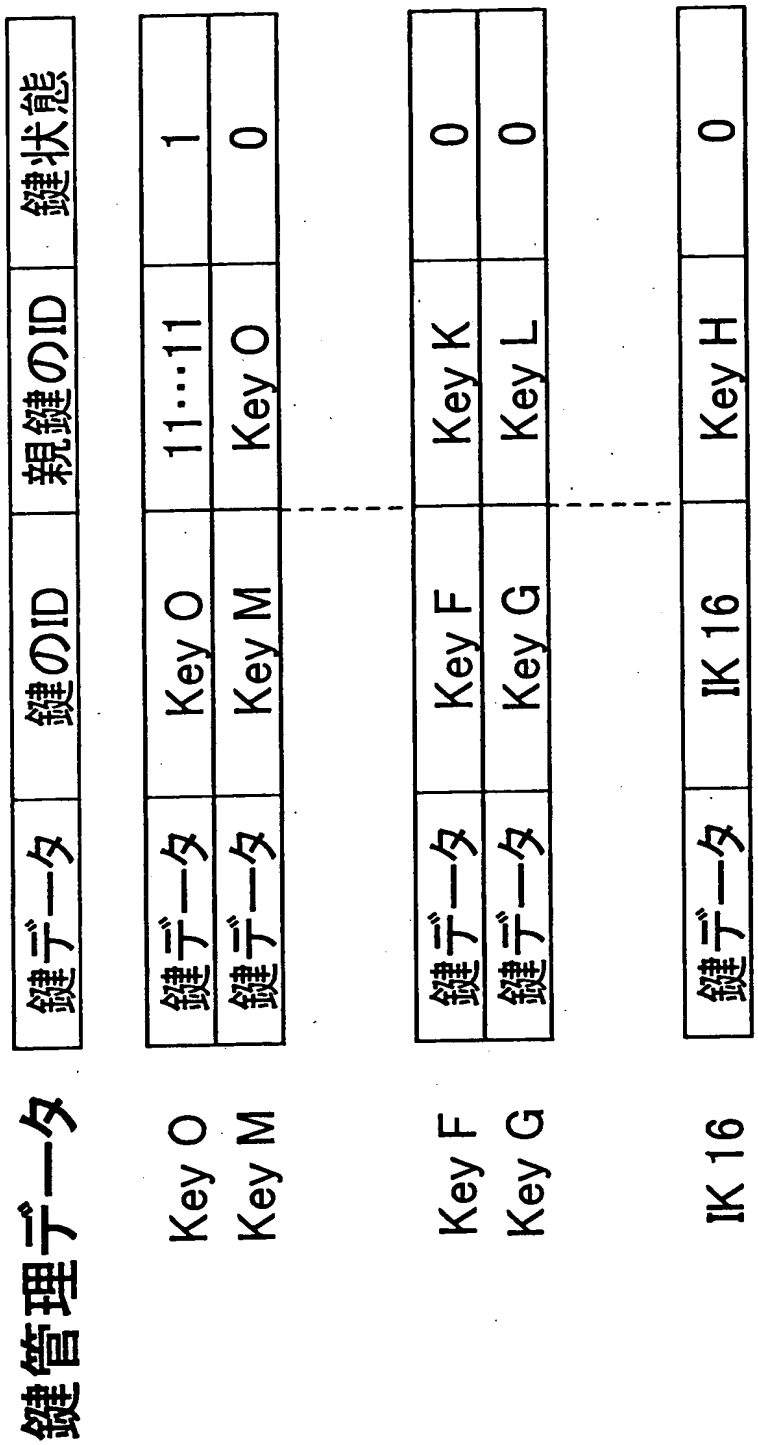
【図６】


レイヤ1
レイヤ2
レイヤ3
Key I
Key J
Key K
Key L
Key A
Key B
Key C
Key D
Key E
Key F
Key G
Key H
ユーザ 1
ユーザ 2
ユーザ 3
ユーザ 4
ユーザ 5
ユーザ 6
ユーザ 7
ユーザ 8
ユーザ 9
ユーザ 10
ユーザ 11
ユーザ 12
ユーザ 13
ユーザ 14
ユーザ 15
ユーザ 16

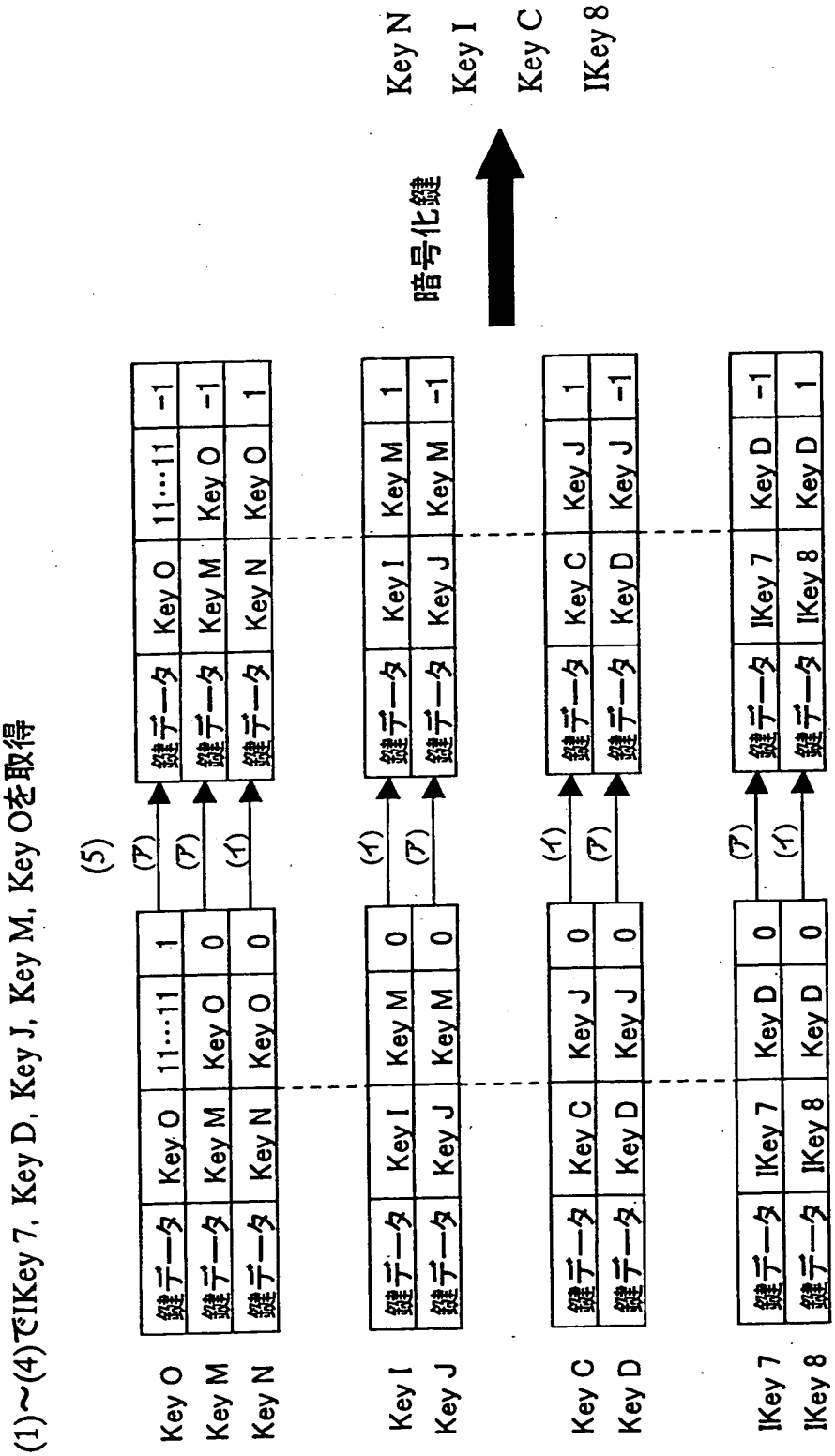
【図７】


Key I
Key A
Key B
Key J
Key C
Key D
Key K
Key E
Key F
Key L
Key G
Key H
レイヤ1
レイヤ2
レイヤ3
ユーザ 1
ユーザ 2
ユーザ 3
ユーザ 4
ユーザ 5
ユーザ 6
ユーザ 7
ユーザ 8
ユーザ 9
ユーザ 10
ユーザ 11
ユーザ 12
ユーザ 13
ユーザ 14
ユーザ 15
ユーザ 16
排除ユーザ

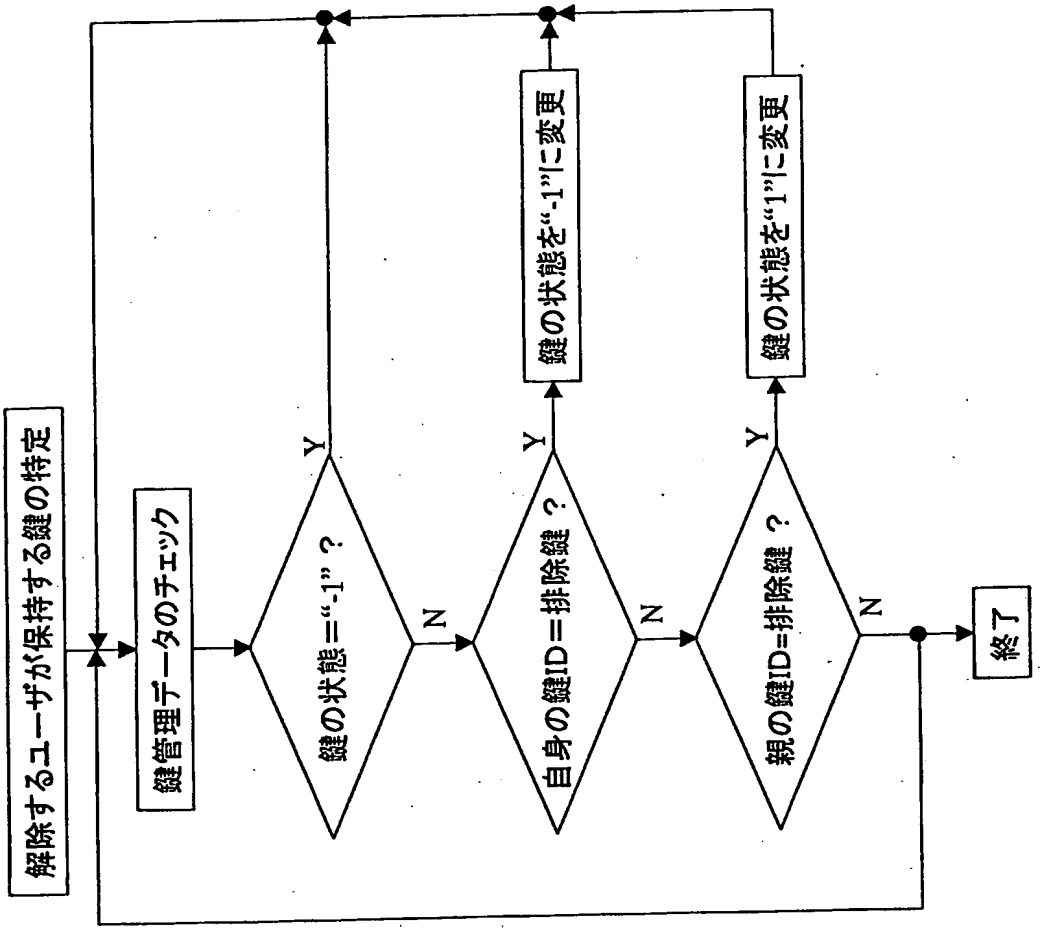
【図８】


鍵管理データ
鍵データ
鍵のID
親鍵のID
鍵状態
鍵データ
Key O
11…11
1
鍵データ
Key M
Key O
0
鍵データ
Key F
Key K
0
鍵データ
Key G
Key L
0
鍵データ
IK 16
Key H
0
Key O
Key M
Key F
Key G
IK 16

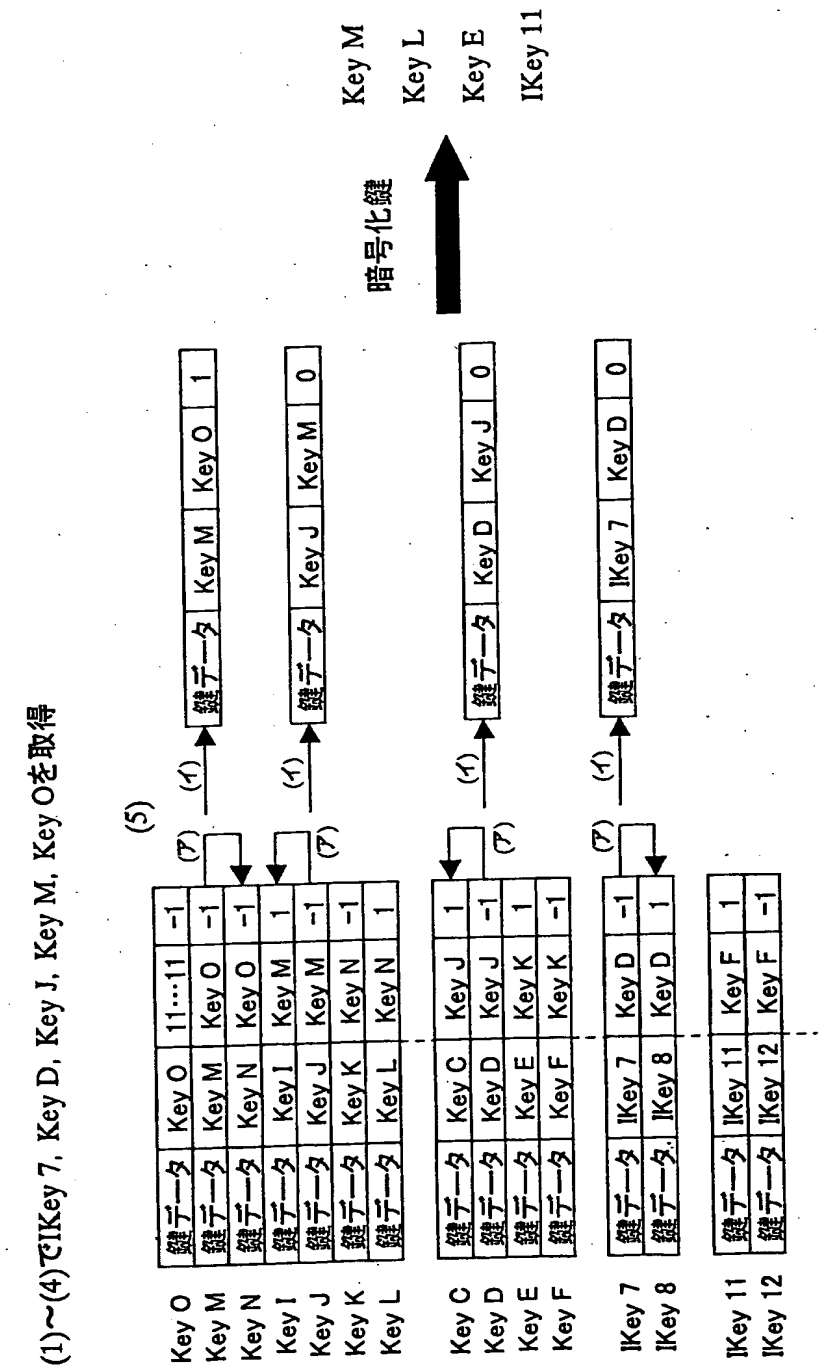
【図９】


(1)～(4)でIKey 7, Key D, Key J, Key M, Key Oを取得
(5)
暗号化鍵
Key N
Key I
Key C
IKey 8
Key O
Key M
Key N
Key I
Key J
Key C
Key D
IKey 7
IKey 8
鍵データ
11…11
1
0
-1

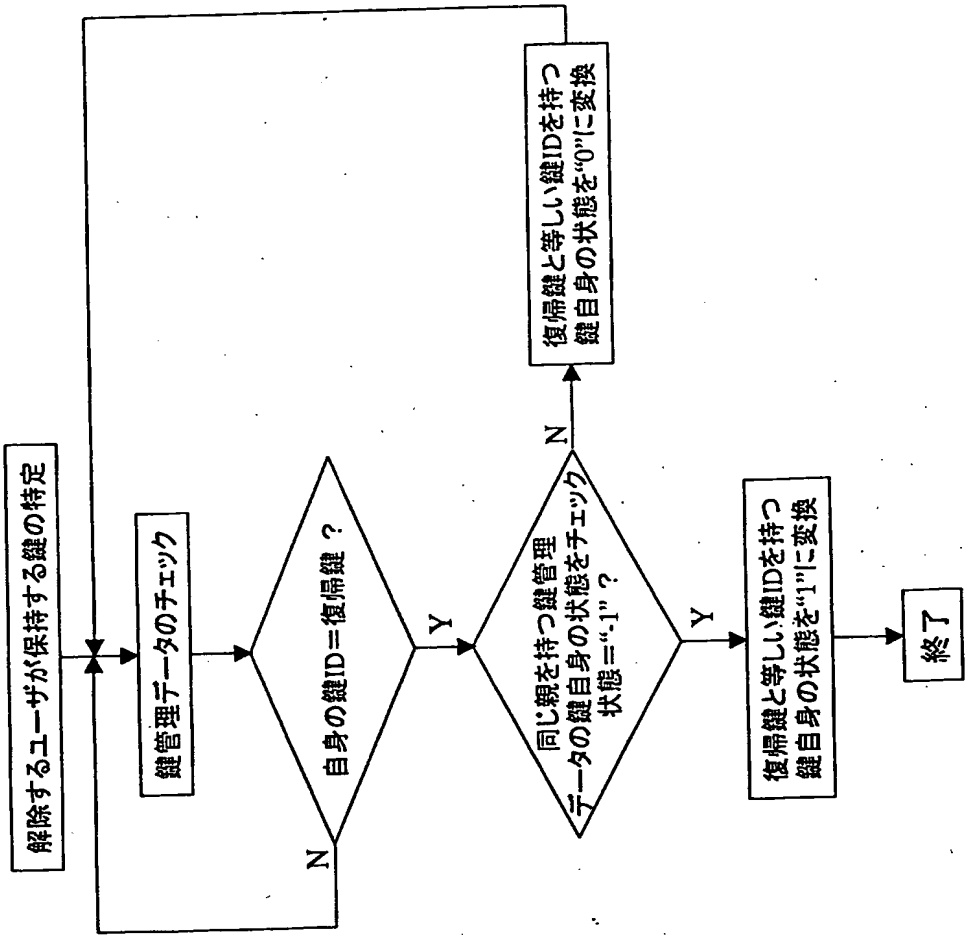
【図１０】


解除するユーザが保持する鍵の特定
鍵管理データのチェック
鍵の状態＝“-1”？
Y
N
自身の鍵ID＝排除鍵？
Y
N
鍵の状態を“-1”に変更
親の鍵ID=排除鍵？
Y
N
鍵の状態を“1”に変更
終了

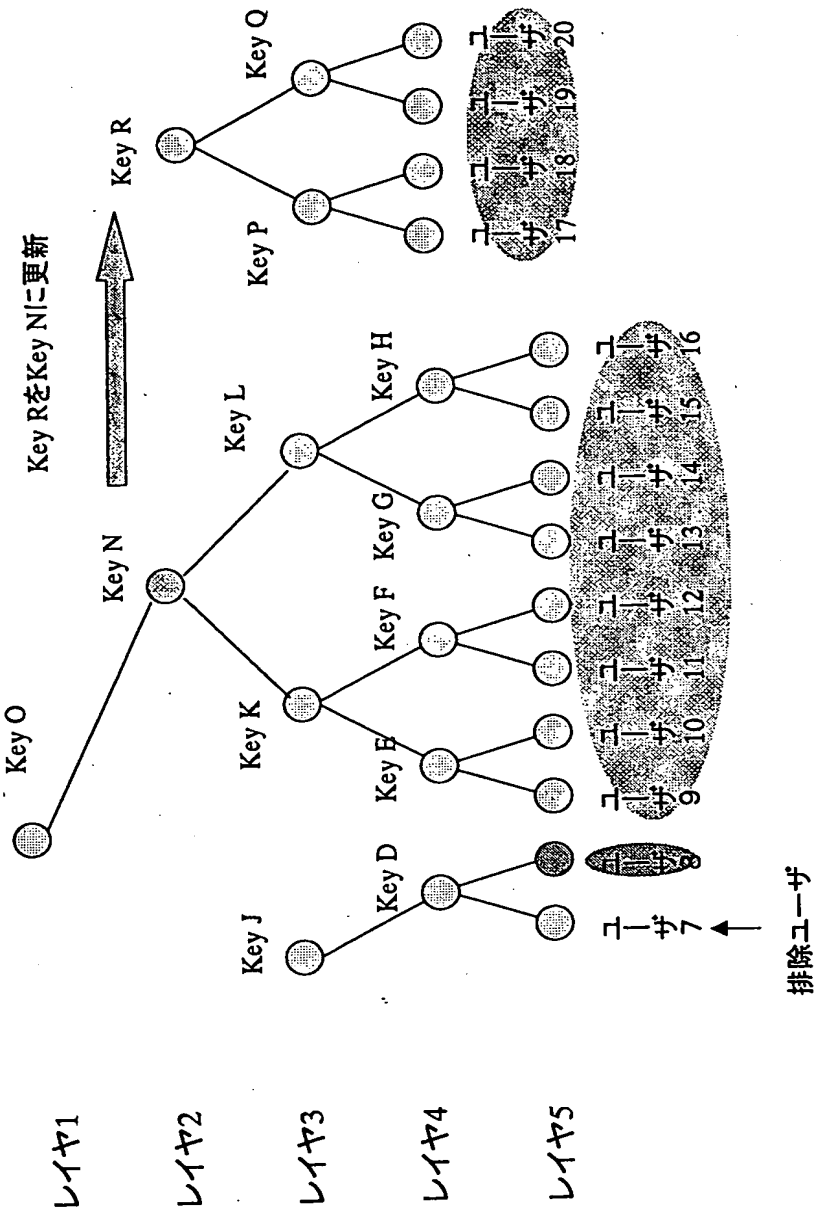
【図１１】


(1)～(4)でIKey 7, Key D, Key J, Key M, Key Oを取得
(5)
暗号化鍵
Key M
Key L
Key E
IKey 11
鍵データ
Key O
11…11
-1
Key M
Key O
-1
Key N
Key O
-1
Key I
Key M
1
Key J
Key M
-1
Key K
Key N
-1
Key L
Key N
1
Key C
Key J
1
Key D
Key J
-1
Key E
Key K
1
Key F
Key K
-1
IKey 7
Key D
-1
IKey 8
Key D
1
IKey 11
Key F
1
IKey 12
Key F
-1
Key O
Key M
Key N
Key I
Key J
Key K
Key L
Key C
Key D
Key E
Key F
IKey 7
IKey 8
IKey 11
IKey 12
(1)
(7)
Key M
Key O
1
Key J
Key M
0
Key D
Key J
0
IKey 7
Key D
0

【図１２】


解除するユーザが保持する鍵の特定
鍵管理データのチェック
自身の鍵ID＝復帰鍵 ？
N
Y
同じ親を持つ鍵管理
データの鍵自身の状態をチェック
状態＝"-1" ？
N
Y
復帰鍵と等しい鍵IDを持つ
鍵自身の状態を"0"に変換
復帰鍵と等しい鍵IDを持つ
鍵自身の状態を"1"に変換
終了

【図１３】


Key O
Key N
Key J
Key K
Key L
Key D
Key E
Key F
Key G
Key H
Key P
Key Q
Key R
Key RをKey Nに更新
ユーザ
ユーザ7
排除ユーザ
レイヤ1
レイヤ2
レイヤ3
レイヤ4
レイヤ5

【書類名】要約書

【要約】

【課題】

映画などの著作物をデジタル化して、DVD等のメディアに格納して配布する方法に関連し、特定のユーザ機器ではもとのデータが獲得できず、それ以外のユーザ機器ではもとのデータが完全に獲得できるような著作権保護データ配送方式を提供する。

【解決手段】

ツリー状配置された暗号鍵を考える。データ配送者はすべてのツリー経路上の鍵とユーザ個別鍵を保持する。各ユーザは対応する個別鍵とその上位の経路上の鍵を保持する。特定ユーザの鍵を無効化する場合、 特定ユーザの持つすべての鍵を除いて、特定ユーザ以外のユーザが最も多く共通に保持する鍵を決定し、さらに、残りのユーザが最も多く共通に保持する鍵を決定し、以下この操作を繰り返し行い、得られた全ての鍵を用いて暗号化を行う。

【選択図】図2

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社